Analysis of Proposed Consent Orders to Aid Public Comment
***In the Matter of Residual Pumpkin Entity, LLC*, and PlanetArt, LLC, File No. 1923209**

The Federal Trade Commission ("Commission") has accepted, subject to final approval, agreements containing consent orders from Residual Pumpkin Entity, LLC ("Residual Pumpkin") and PlanetArt, LLC ("PlanetArt") (collectively, "Respondents").

The proposed consent orders ("Proposed Orders") have been placed on the public record for thirty (30) days for receipt of comments by interested persons. Comments received during this period will become part of the public record. After thirty (30) days, the Commission will again review the agreements and the comments received and will decide whether it should withdraw from the agreements and take appropriate action or make final the Proposed Orders.

This matter involves Respondents' data security and privacy practices. Respondent Residual Pumpkin owned CafePress until September 2020, when Residual Pumpkin sold CafePress to Respondent PlanetArt. The CafePress website allows users, known as shopkeepers, to earn commissions from sales of merchandise offered to consumers. CafePress collected information such as names, email addresses, telephone numbers and—from shopkeepers—Social Security numbers ("Personal Information"). CafePress claimed to keep this information safe, but in fact failed to provide reasonable security. For example, CafePress failed to: guard against well-known and reasonably foreseeable threats, such as SQL injection and cross-site scripting attacks; encrypt Social Security numbers; and implement a process for receiving and addressing third-party security vulnerability reports. CafePress also claimed to adhere to principles set forth in the EU-U.S. and Swiss U.S. Privacy Shield frameworks, specifically that it would honor user requests to delete data and user choices about how email addresses would be used. Instead, CafePress failed to delete Personal Information when it was requested to do so and sent marketing emails to nearly all its consumers, even those who had not opted in to receive such messages. As a result of CafePress' data security practices, consumers' Personal Information was stolen and sold on the dark web. CafePress learned of the breach but failed to notify affected consumers. After some shopkeepers learned of the breach and closed their accounts, CafePress withheld up to $25 in payable commissions from each of those shopkeepers.

The complaint alleges that Respondents violated Section 5(a) of the FTC Act by: (1) misrepresenting the measures CafePress took to protect Personal Information; (2) misrepresenting the steps CafePress took to secure consumer accounts following security incidents; (3) failing to employ reasonable data security practices; (4) misrepresenting how CafePress would use email addresses; (5) misrepresenting CafePress' adherence to the Privacy Shield frameworks; (6) misrepresenting whether CafePress would honor deletion requests; and (7) unfairly withholding commissions payable to shopkeepers.

The Proposed Orders contain provisions designed to prevent Respondents from engaging in the same or similar acts or practices in the future.

Summary of Proposed Order with Residual Pumpkin

Part I prohibits Residual Pumpkin from misrepresenting: (1) privacy and security measures it takes to prevent unauthorized access to Personal Information; (2) the extent to which Residual Pumpkin is a member of any privacy or security program sponsored by a government, self-regulatory, or standard-setting organization; (3) privacy and security measures to honor users' privacy choices; (4) information deletion and retention practices; and (5) the extent to which it maintains and protects the privacy, security, availability, confidentiality, or integrity of Personal Information.

Part II requires Residual Pumpkin to establish and implement, and thereafter maintain, a comprehensive information security program ("Security Program") that protects the privacy, security, confidentiality, and integrity of Personal Information.

Part III requires Residual Pumpkin to obtain initial and biennial data security assessments for 20 years.

Part IV requires Residual Pumpkin to disclose all material facts to the assessor and prohibits Residual Pumpkin from misrepresenting any fact material to the assessment required by Part II.

Part V requires Residual Pumpkin to submit an annual certification from a senior corporate manager (or senior officer responsible for its Security Program) that Residual Pumpkin has implemented the requirements of the order and is not aware of any material noncompliance that has not been corrected or disclosed to the Commission.

Part VI requires Residual Pumpkin to notify the Commission of a "Covered Incident" within thirty days of discovering such incident.

Parts VII and **VIII** require Residual Pumpkin to pay to the Commission $500,000 and describe the procedures and legal rights related to that payment.

Part IX requires Residual Pumpkin to provide customer information to enable the Commission to administer consumer redress.

Part X requires Residual Pumpkin to submit an acknowledgement of receipt of the order, including all officers or directors and employees having managerial responsibilities for conduct related to the subject matter of the order, and to obtain acknowledgements from each individual or entity to which a Residual Pumpkin has delivered a copy of the order.

Part XI requires Residual Pumpkin to file compliance reports with the Commission and to notify the Commission of bankruptcy filings or changes in corporate structure that might affect compliance obligations.

Part XII contains recordkeeping requirements for accounting records, personnel records, consumer correspondence, advertising and marketing materials, and claim substantiation, as well as all records necessary to demonstrate compliance with the order.

Part XIII contains other requirements related to the Commission's monitoring of Respondent's order compliance.

Part XIV provides the effective dates of the order, including that, with exceptions, the order will terminate in twenty (20) years.

Summary of Proposed Order with PlanetArt

Part I prohibits PlanetArt from misrepresenting: (1) privacy and security measures it takes to prevent unauthorized access to Personal Information; (2) the extent to which PlanetArt is a member of any privacy or security program sponsored by a government, self-regulatory, or standard-setting organization; (3) privacy and security measures to honor users' privacy choices; (4) information deletion and retention practices; and (5) the extent to which it maintains and protects the privacy, security, availability, confidentiality, or integrity of Personal Information.

Part II requires PlanetArt to establish and implement, and thereafter maintain, a comprehensive information security program that protects the privacy, security, confidentiality, and integrity of Personal Information.

Part III requires PlanetArt to obtain initial and biennial data security assessments for 20 years.

Part IV requires PlanetArt to disclose all material facts to the assessor and prohibits PlanetArt from misrepresenting any fact material to the assessment required by Part II.

Part V requires PlanetArt to submit an annual certification from a senior corporate manager (or senior officer responsible for its Security Program) that PlanetArt has implemented the requirements of the order and is not aware of any material noncompliance that has not been corrected or disclosed to the Commission.

Part VI requires PlanetArt to notify the Commission of a "Covered Incident" within thirty days of discovering such incident.

Parts VII requires PlanetArt to provide notice to consumers to inform them of the breach and the settlement with the FTC.

Part VIII requires PlanetArt to submit an acknowledgement of receipt of the order, including all officers or directors and employees having managerial responsibilities for conduct related to the subject matter of the order, and to obtain acknowledgements from each individual or entity to which a PlanetArt has delivered a copy of the order.

Part IX requires PlanetArt to file compliance reports with the Commission and to notify the Commission of bankruptcy filings or changes in corporate structure that might affect compliance obligations.

Part X contains recordkeeping requirements for accounting records, personnel records, consumer correspondence, advertising and marketing materials, and claim substantiation, as well as all records necessary to demonstrate compliance with the order.

Part XI contains other requirements related to the Commission's monitoring of PlanetArt's order compliance.

Part XII provides the effective dates of the order, including that, with exceptions, the order will terminate in 20 years.

The purpose of this analysis is to facilitate public comment on the Proposed Orders, and it is not intended to constitute an official interpretation of the complaint or Proposed Orders, or to modify the Proposed Orders' terms in any way.